CLAIMS

What is claimed is:

1. An integrated intrusion detection method comprising:

gathering information from a plurality of different types of intrusion detection sensors;

processing said information, wherein said processing provides a consolidated correlation of said information;

assigning a response corresponding to said information; and

implementing said response.

2. An integrated intrusion detection method of Claim 1 wherein said information includes intrusion detection alerts.

3. An integrated intrusion detection method of Claim 2 further comprising centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors.

4. An integrated intrusion detection method of Claim 3 wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors.

5. An integrated intrusion detection method of Claim 2 wherein said intrusion detection alerts are correlated based upon various alert attributes.

6. An integrated intrusion detection method of Claim 2 wherein said response conforms to an enterprise wide strategy.

7. An integrated intrusion detection method of Claim 1 further comprising managing said detection sensors.

8. A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions comprising:

a data collection module for receiving information from a plurality of different types of security examination components, wherein said information indicates potential security issues;

an integration module for integrating said information in a network application management platform;

a reaction determination module for determining appropriate response to indication of said potential security issues; and

a reaction direction module for directing said response.

9. A computer usable storage medium of Claim 8 wherein said information includes intrusion detection system alert data.

10. A computer usable storage medium of Claim 8 wherein said integration module selects appropriate hooks in an intrusion detection system.

11. A computer usable storage medium of Claim 8 wherein said data collection module logs alerts from said plurality of different types of security examination components.

12. A computer usable storage medium of Claim 8 wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface.

13. A computer usable storage medium of Claim 8 wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path.

14. A computer usable storage medium of Claim 8 wherein said integration module utilizes a network application management platform to log information.

15. A computer usable storage medium of Claim 14 wherein:

an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts;

an open view operation log file encapsulator handles system log based alerts; and

an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism.

16. A computer usable medium of Claim 14 wherein a secure open view template configuration is utilized to log information and the one message group is configured

for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors.

17. An intrusion detection central system comprising:

a bus for communicating information;

a processor coupled to said bus, said processor for processing said information including instructions for coordinating security information from a plurality of different security intrusion attempt identification components; and

a memory coupled to said bus, said memory for storing said information, including instructions for coordinating security information from a plurality of different security intrusion attempt identification components.

18. An intrusion detection central system of claim 17 wherein said instructions include security management instructions implemented on a network application management platform.

19. An intrusion detection central system of claim 18 further comprising a central console for interfacing with said network application management platform.

20. An intrusion detection central system of claim 17 wherein said instructions include incident reaction instructions.